## REMARKS

Claims 1-88 were submitted for examination. In this Office Action, the Examiner has rejected Claims 1-5, 10-25 and 28-47 under 35 USC 102(e) as being anticipated by Pensak et al (US Patent No.: 6,339,825) and Claims 6-9, and 26-27 under 35 USC 103(a) as being unpatentable over Pensak et al in view of Ozog et al (US Application Publication 2003/0033528. The two cited references are referred to hereinafter as Pensak and Ozog, respectively, hereinafter.

The Examiner is thanked for his thoughtful and timely review of the application. In the forgoing amendments, Claims 16, 63 and 81 have been cancelled and Claims 1, 30, 31, 36, 41-43, 48, 67 and 78 have been amended. As a result, Claims 1-15, 17-62, 64-80 and 82-88 are now pending. Reconsideration of the pending claims is respectfully requested.

Pensak was provided by the Applicants and deemed most closely related to the subject matter, or subject matters of the pending claims. However, the Applicants do not consider that Pensak is prior art, many recited features in the pending claims are neither taught nor suggested in Pensak.

As shown in FIG. 1 and the description thereof (Col. 2, lines 15-48) in Pensak, a document 110 is encrypted with an encryption key(s) provided by the remote server 106. The encrypted document is then registered with the remote server 106 and associated with a set of access policies with the encryption key so that only selected users 116 under selected circumstances may view the encrypted document. Lines 50-62 of Col. 2 in Pensak continues the description of what the remote server 106 provides, including providing description keys 118 and associated access policies. In brief summary, Pensak requires a server to manage the keys and access policies and hence the server must be connected or consulted before the encrypted document can be revealed to an application (e.g., a viewing tool 104 in FIG. 1).

In contrast, the once-amended Claim 1 recites:

...
the electronic data is secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;
authenticating the user according to the identifier; and
activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

(*emphasis added*)

In other words, the electronic data is secured in a format having two portions (i.e. security information portion and the encrypted data portion), where the security information portion includes the file key and the access rules. There are several distinct features in the once-amended Claim 1 that are not taught or suggested in Pensak. Only three are discussed herein for distinctions.

First, Pensak keeps the decryption key in a remote server that also generates an encryption while Claim 1 recites that a file key (e.g., a decryption key) is included in the file itself. Second, Pensak keeps the access rules in a remote server as well while Claim 1 recites that the access rules is included in the file itself. Third, the file key will have to be retrieved from the remote server to decrypt the encrypted document in Pensak while Claim 1 recites that the file key is retrieved from the file itself and decrypt the encrypted data portion. Accordingly, The Applicants submit that Pensak neither teaches nor suggests, in fact, teaches away from the features recited in the once-amended Claim 1.

Ozog teaches techniques to verify and validate the identity of a requester using digital certificate but teaches nothing about how a file is secured and accessed by way of policies or rules. In particular, Ozog has neither taught nor suggested using access rules expressed in a markup language to protect a file key that is itself encrypted and has been used to encrypt a file being secured. Accordingly, the Applicants submit Claim 1 and dependent claims 2-15 and 17-30 shall be allowable over Pensak or Ozog, viewed alone or in combination. Reconsideration of Claim 1-15 and 17-30 is respectfully requested.

Claim 31 has also been amended to further distinguish from the cited references. In addition to the distinct features presented above over the cited references, Claim 31 further recites "determining from the security information if the user has necessary access privilege to access the encrypted data portion without consulting with another machine" (*emphasis added*), which means that a secured file may be accessed offline, namely no server needs to be consulted with. In contrast, Pensak must have the viewing toll 104 to send a request to the remote server 106 and in return to get the decryption (file) key 118, detailed in FIG. 1 in Pensak. Evidently, the combined features recited in the once-amended Claim 31 are neither taught nor suggested in Pensak or Ozog, viewed alone or in combination. Accordingly, the Applicants respectfully request the Examiner to reconsider Claims 31-46.

In addition to the distinct features presented above over the cited references, Claim 47 recites that "... a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place; an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data..." In other words, a secured file itself carries the encrypted security information, a part of the secured file including the encrypted security information is transported to a server wherein the encrypted security information is decrypted with a user key in the server. Pensak requires that the security information be maintained in a server and neither teaches nor suggests that the security information is encrypted with another (user) key. Accordingly, the Applicants submit that Claim 47 shall be allowable over Pensak and respectfully request the Examiner to reconsider Claims 47.

Claims 48-62 and 64-80, and 82-88 are rejected with similar reasons in the Office Action. The Applicants have amended Claims 48, 67 and 78 to clearly distinguish from the cited references and wish to apply the reasons presented above to support Claims 48-62, 64-80, and 82-88. Accordingly, Claims 48-62, 64-80, and 82-88 are believed equally patentable over the cited references, viewed alone or in combination.

In view of the above amendments and remarks, the Applicants believe that Claims 1-15, 17-62, 64-80 and 82-88 shall be in condition for allowance. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on May 20, 2003.

Faxed to (703)305 -7687

Name: Joe Zheng

Signature: JZheng

Respectfully submitted;

JZheng

Joe Zheng
Reg. No.: 39,345